Headquarters
U.S. Army Armor Center and Fort Knox
Fort Knox, Kentucky 40121-5000
12 April 2000

*Fort Knox Reg 25-70

Information Management

PROCEDURES FOR THE ENTRY OF INFORMATION INTO THE FORT KNOX WORLD WIDE WEB (WWW) SITE/INTERNET AND USE OF FORT KNOX COMMUNICATIONS RESOURCES

Summary. This regulation provides guidance and procedures for the entry of information into the Fort Knox WWW Site/INTERNET and use of Fort Knox communications resources.

Applicability. This regulation applies to all major activities, staff offices, directorates, departments, and Partners in Excellence, this headquarters.

Suggested Improvements. The proponent of this regulation is the Director, Directorate of Information Management. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, USAARMC and Fort Knox, ATTN: ATZK-IM, Fort Knox, KY 40121-5520.

1. References.

a. AR 25-1, 15 Feb 00, Army Information Management.

b. AR 380-19, 27 Feb 98, Information Systems Security.

c. TRADOC Regulation 25-70, 1 Jul 97, Network Services.

d. TRADOC Pamphlet 25-70, 8 Sep 97, Homepages and Websites.

2. Due to security and legal ramifications, careful consideration must be given before entering any information into the Fort Knox WWW Site/INTERNET. Appendix A to this regulation provides guidance and procedures for the entry of information into the Fort Knox WWW Site/ INTERNET. This appendix outlines the different categories of information and their releasability into the Fort Knox WWW Site/INTERNET.

3. As stated in Appendix A, Unclassified Public Domain Information can be entered into the Fort Knox WWW Site and the INTERNET upon appropriate coordination and approval of the activity's commander/director. Classified Military Information (CONFIDENTIAL, SECRET, TOP SECRET) will never be entered into the Fort Knox WWW Site or the INTERNET under any circumstances. Controlled Unclassified Information will not be placed on the INTERNET, but may, after appropriate coordination and approval of G3/DPTM Security Division, PAO, and SJA, be placed on the Fort Knox WWW Site.

4. The INTERNET provides a tremendous resource of information exchange and other communications through such vehicles as mail list servers, data bases, files, and web sites. Appendix B to this regulation contains guidance on the use of Fort Knox communications resources used to access this information. These resources include, but are not limited to: government-owned PCs, networks, routers, gateways, modems, telephone lines, and software. This policy must be adhered to in order to prevent the misuse of these resources.

5. The Fort Knox WWW Site/INTERNET will be the only site for USAARMC and Fort Knox. Subordinate organizations and activities will not create their own INTERNET sites. Before placing any information on the Fort Knox WWW Site/INTERNET, coordination must be made with G3/DPTM Security Division, PAO, and SJA. Format for approval document is located at Annex 1 to Appendix A. Only after approval from the three above-named agencies will the DOIM Webmaster place this information on the WWW Site. All major changes to previously approved content must also follow this approval process. Graphical enhancements, typographical corrections, and original design will be coordinated with the DOIM Webmaster, phone 4-1805.

FOR THE COMMANDER:

OFFICIAL:
GEORGE EDWARDS
Colonel, AR
Garrison Commander

ROBERT L. BROOKS
Director, Information Management

DISTRIBUTION:
A plus
50 – ATZK-IM
5 – ATSB-OPL

CF:
DCG, USAARMC

APPENDIX A

RELEASABILITY GUIDE FOR THE FORT KNOX WORLD WIDE WEB SITE

Background. There are three major categories of military information: Unclassified Public Domain Information, Classified Military Information (CMI), and Controlled Unclassified Information (CUI). Their descriptions and their releasability on the Fort Knox World Wide Web Site and the INTERNET follows.

1. **UNCLASSIFIED PUBLIC DOMAIN INFORMATION**. This information is releasable to the public; can be placed on the Fort Knox World Wide Web Site and the INTERNET upon appropriate coordination and the approval of the activity's commander or director (see appendix A for sample format). This information does not qualify for the status of CMI or CUI as described below. This information is deemed to be actually or potentially in the public domain, that is, suitable for release to the public at large. "The public at large" encompasses not only citizens of the U.S. and immigrant aliens, but also citizens of all foreign countries. Below are examples of this information.

a. General information about Fort Knox that has been released to the public.

EXAMPLES

Command briefings (unless of a sensitive nature).
Community events calendar.
Welcome packets.
DBO club activities.
Town Hall meetings.
Courts-martial results.

b. Training information that has been given to foreign government representatives.

EXAMPLES

Course POIs (unless of a sensitive nature)
Class dates.
Range schedules.

c. Conferences, demonstrations, and dedications.

EXAMPLES

Armor Conference.
American Defense Preparedness Association (ADPA) Conference.

Live fire demonstrations.
Building dedications.

d. Contract activities open for public solicitation.

2. **CLASSIFIED MILITARY INFORMATION**. (Reference: AR 380-5, 25 Feb 88, Department of the Army Information Security Program.) This information is not releasable for placement on the Fort Knox World Wide Web Site or the INTERNET under any circumstances. CMI is information that is of such sensitivity that it requires special protection. According to its degree of sensitivity, CMI is identified by a level of security classification: CONFIDENTIAL, SECRET, or TOP SECRET. CMI information will never be placed on the Fort Knox World Wide Web Site or the INTERNET. The transmission of CMI will only be accomplished on an accredited system protected by an approved encryption product.

3. **CONTROLLED UNCLASSIFIED INFORMATION**. This information is not releasable for placement on the INTERNET. CUI is information that does not require the degree of protection afforded by the application of security classification. Nevertheless, certain unclassified information may be of such sensitivity as to warrant placing a degree of control over its use and dissemination. CUI normally falls into one of the following categories.

a. PRIVACY ACT INFORMATION. (Reference: AR 340-21, 5 Jul 85, The Army Privacy Program, implements the Privacy Act of 1974, 5 U.S.C. 552a, as amended.) Definition: Personal information, described as "information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life." This information cannot be released to the public because its release would result in the violation of the personal privacy of the individual to whom it pertains, and possible litigation against the government or government personnel.

EXAMPLES

Social security numbers.
Date of birth.
Home addresses.
Home phone numbers.
Medical history/records.
Personnel actions/files.
Personal security investigations.
Payroll/financial records.
Law enforcement/criminal investigations.
Names of military members assigned to sensitive, routinely-deployable units.
EEO actions.
Nonjudicial punishment or administrative discipline.

b. FOR OFFICIAL USE ONLY INFORMATION. (Reference: AR 25-55, 14 Apr 97, The Department of the Army Freedom of Information Act Program, implements the Freedom of Information Reform Act of 1986, P.L. 99-570, 5 U.S.C. 552b). Definition: Information that has not been given a security classification, but can be withheld from the public based on the remaining eight statutory exemptions under the Freedom of Information Act (FOIA). This information should be marked correctly, i.e., bottom of outside of front cover, first page, each page containing protected information, and outside of last page or back cover.

c. FOIA EXEMPT INFORMATION. (Reference: AR 25-55). Definition: That information which falls under the nine statutory exemptions under the FOIA; below is a list of these exemptions.

(1) Exemption 1 - Classified. Information given the classification of CONFIDENTIAL, SECRET, or TOP SECRET.

(2) Exemption 2 - Internal rules and practices.

(a) Rules, regulations, orders, manuals, directives, and instructions whose release would allow circumvention of these records.

1. Operating rules, guidelines, and manuals for DOD investigators, inspectors, auditors, or examiners that must remain privileged in order for the DOD Component to fulfill a legal requirement.

EXAMPLES

Guidelines for conducting particular investigations.
Guidelines for conducting post-investigative litigation.
Guidelines for identifying law violators.
Studies of agency practices and problems pertaining to undercover agents.
Vulnerability assessments.
Computer security plans.
Agency audit guidelines.
Security techniques used in penal institutions.
Classification manuals detailing categories of information classified and their classification levels.
Internal documents used to staff operational decisions.
Schedules of special tests and events (equipment tests, field exercises (MBBL/ARI), etc.)

2. Personnel and other administrative matters, such as examination questions and answers used in training courses or in the determination of the qualification of candidates for employment, entrance on duty, advancement, or promotion.

EXAMPLES

Crediting plans used in employment processes.
Merit promotion rating plans.
Agency testing materials.
Training publications (FMs, TMs, lesson plans, etc.).

(b) Trivial and housekeeping records that hold no legitimate public interest or benefit in release.

EXAMPLES

Rules of employees' use of parking facilities.
Regulation of lunch hours.
Statements of policy pertaining to sick leave.
Administrative data such as file numbers, mail routing stamps, data processing notations, etc.

(c) Negotiation and bargaining techniques, practices, and limitations.

(3) Exemption 3 - Information exempted by other statutes.

EXAMPLES

National Security Agency Information Exemption, P.L. 86-36, Section 6.
Patent Secrecy, 35 U.S.C. 181-188.
Restricted Data and Formerly Restricted Data, 42 U.S.C. 2162.
Communication Intelligence, 18 U.S.C. 798.
Authority to Withhold From Public Disclosure Certain Technical Data, 10 U.S.C. 130 and DOD Directive 5230.25.
Confidentiality of Medical Quality Records: Qualified Immunity Participants, 10 U.S.C. 1102.
Physical Protection of Special Nuclear Material: Limitation on Dissemination of Unclassified Information, 10 U.S.C. 128.
Protection of Intelligence Sources and Methods, 50 U.S.C.403(d)(3).
Inspector General Act, 5 U.S.C., Appendix 3.

(4) Exemption 4 - Trade secrets, commercial/financial information given to the government (by nongovernmental entities) in confidence.

EXAMPLES

Business sales statistics.

Research data.
Technical designs and proposals.
Customer and supplier lists.
Profit and loss data.
Overhead and operating costs.
Information on financial condition.
Labor costs.
Information on competitive vulnerability.
Names of consultants and subcontractors.
Performance, cost, and equipment information.
Shipper and importer information.
Currently unannounced and future products.
Pricing strategy.
Sales and distribution data.
Bids for contracts.
Grant or loan applications.

(5) Exemption 5 - Interagency, intra-agency communications.

(a) Internal advice, recommendations, and subjective evaluations, as contrasted with factual matters, that are reflected in records pertaining to the decision-making process of an agency; records pertaining to the deliberative process privilege, attorney-client privilege, and the attorney work-product privilege.

EXAMPLES

Nonfactual portions of staff papers.
Advice, suggestions, or evaluations prepared on behalf of DOD by individual consultants or by boards, committees, etc. formed to obtain advice and recommendations.
Nonfactual portions of evaluations by DOD Component personnel of contractors and their products.
Information of a speculative, tentative, or evaluative nature.
Proposed plans to procure, lease, or otherwise acquire and dispose of materials, real estate, facilities or functions, when such information would provide undue or unfair competitive advantage to private personal interests or impede legitimate Government interests.
Trade secrets or other confidential research development owned by the Government, where Premature release is likely to affect the Government's negotiating position or commercial interest.
Portions of official reports of inspection, IG reports, audits, investigations, or surveys pertaining to safcty, security, or the internal management, administration, or operation of one of more DOD Components when these records have traditionally been treated by the courts as privileged against disclosure in litigation.

Planning, programming, and budgetary information involved in the defense planning and resource allocation process.

(b) Deliberative process privilege. Used to prevent injury to the quality of agency decisions by:

Encouraging open, frank discussions on matters of policy.
Protecting against premature disclosure of proposed policies before adoption.
Protecting against public confusion resulting from disclosure of reasons and rationales that were not in fact ultimately grounds for an agency's action.

(c) Attorney work-product privilege. Protects documents and other memoranda prepared by an attorney in contemplation of litigation.

(d) Attorney-client privilege. Protects confidential communications between an attorney and client relating to a legal matter for which the client has sought professional advice.

(6) Exemption 6 - Personnel, medical, similar Privacy Act protected files. SEE PRIVACY ACT INFORMATION ABOVE.

(7) Exemption 7 - Investigative files compiled for law enforcement. Records that could result in:

Interference with enforcement proceedings.
Deprive a person of the right to a fair trial or impartial adjudication.
Constitute an unwarranted invasion of personal privacy of a living person or surviving family members.
Disclosure of identity of confidential source.
Disclosure of information from a confidential source obtained by criminal law enforcement authority in a criminal investigation or agency conducting lawful national security intelligence investigation.
Would disclose techniques and procedures for law enforcement investigations or prosecutions if such disclosure could result in circumvention of the law.
Could reasonably be expected to endanger life or physical safety of any individual.

EXAMPLES

Witness statements.
Material developed in course of investigation.
Material prepared in connection with government litigation or adjudicative proceedings.
Identity of firms or individuals being investigated for alleged irregularities involving contracting with the DOD (Army) when no indictment has been obtained nor any civil action filed against them by the United States.

Information obtained in confidence.

(8)Exemption 8 - Those contained in or related to examination, operation, or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions.

EXAMPLES

Bank examination reports.
Internal bank or credit union memoranda.

(9)Exemption 9 - Those containing geological and geophysical information and data (including maps) concerning wells. Well information of a technical or scientific nature.

EXAMPLES

Subterranean maps showing exact location of privately-owned oil and natural gas wells or other underground natural resources.
Natural resource mining.

d. UNCLASSIFIED INFORMATION THAT REQUIRES SPECIAL HANDLING: I.E., ENCRYPT FOR TRANSMISSION ONLY (EFTO), LIMITED DISTRIBUTION (LIMDIS), SCIENTIFIC AND TECHNICAL INFORMATION PROTECTED UNDER THE TECHNOLOGY TRANSFER LAWS.

(1) EFTO. The classification marking unclassified EFTO is not authorized for use on messages originated within the U.S. Army. This marking is used by the U.S. Air Force.

(2) LIMDIS. This pertains to classified information concerning specific projects or subjects that must received limited distribution. As with any other classified information, this type of information WILL NOT be placed on INTERNET.

(3) Dissemination of scientific and technical information. (Reference: AR 70-11, 31 Mar 86, Dissemination of Scientific and Technical Information; and AR 70-31, 10 Mar 86, Standards for Technical Reporting). Information that relates to research, development, engineering, test, evaluation, production, operation, maintenance or employment of military equipment systems. Distribution restriction notices (advising that the information is not for public dissemination) are placed on publications containing technical information.

EXAMPLES

Engineering drawings and plans.
Engineering standards and instructions.

Engineering specifications.
Technical drawings and blueprints.
Technical manuals.
Computer software.
Other technical information that can be used or adapted for use to design, engineer, produce, operate, repair/overhaul, or reproduce any military equipment or technology concerning such equipment.

d. OPERATIONS SECURITY (OPSEC). (Reference: AR 530-1, 3 May 95, Operations Security). OPSEC measures will be applied to activities, either CLASSIFIED or UNCLASSIFIED which require that essential secrecy and surprise be retained. These activities include: logistical support functions; research, development, test, and evaluation; design, engineering, contracting, procurement, and deployment systems; development and execution of policies, procedures, doctrine, strategy, tactics and techniques; and storage and movement of ordnance. Information requiring OPSEC procedures will never be considered public domain information.

EXAMPLES

Equipment status reports.
Equipment test results.
Results of field training exercises.
Research and design specifications.
Mobilization planning.
Ammunition storage and movement plans and procedures.
Fielding plans for new equipment.
Tactical doctrine development.

f. MILITARY LISTINGS. If listings of military/civilian personnel are entered into the INTERNET, the only information we generally release is name, rank/grade, and unit/duty address. Other information is releasable, but only when requested. On any listing that shows name and unit/duty address, we delete the names of those assigned to sensitive, routinely-deployable units (703d Ordnance Company (EOD) is the only one located at Fort Knox at present) and the names of those who have the following suffixes attached to their MOS: A, B, D, E, G, M, U, and V; this release is prohibited because it may cause the individuals or their family to be targeted for terroristic threatening. Accordingly, when a request for a staff directory is received from a nongovernment requester, we delete the names of those assigned to the 703d Ordnance Company (EOD) before release.

ANNEX 1 TO APPENDIX A

(OFFICE SYMBOL) (25)

MEMORANDUM THRU

Director, G3/DPTM, ATTN: ATZK-PTF

Public Affairs Officer, ATTN: ATZK-PAO

Staff Judge Advocate: ATTN: ATZK-JAA

FOR Director, DOIM, ATTN: ATZK-IMA-S (Webmaster)

SUBJECT: Request for Entry of Information into the Fort Knox World Wide Web (WWW) Site/INTERNET

1. Purpose. To submit the enclosed information for entry into the Fort Knox WWW Site/INTERNET.

SUBJECT:
DATE:
DISTRIBUTION RESTRICTION STATEMENT (if applicable):

2. Recommendation. That the enclosed information be approved for entry into the WWW Site/INTERNET.

3. Justification. (STATE JUSTIFICATION)

4. Point of contact is (NAME), phone (X-XXXX).

Encl(s) (COMMANDER'S/DIRECTOR'S SIGNATURE)

APPENDIX B

OFFICIAL AND AUTHORIZED USES OF TELECOMMUNICATIONS AND COMPUTING SYSTEMS

1. The use of DOD and other government telephone systems, e-mail and other systems (including the Internet) are limited to the conduct of official business or other authorized uses. Commanders and supervisors at all levels will make anyone using Government telecommunications systems aware of permissible and unauthorized uses. Local policies and procedures will be promulgated, as necessary, to avoid disruptions of telecommunications systems. The DODD 5500.7-R, Joint Ethics Regulation, Section 2-301 serves as the basis for Army policy on the use of telecommunications and computing systems. Users will abide by these restrictions to prevent security compromises and to avoid disruptions of Army communications systems.

2. All communications users must be aware of security issues and their consent to monitoring for all lawful purposes, of restrictions on transmitting classified information over unsecured communications systems, of prohibitions regarding release of access information such as passwords, and of the need for care when transmitting other sensitive information.

3. Commanders recover toll charges, as practical, for unofficial/unauthorized personal telephone calls placed on official telephones by personnel in their organizations. Persons making unauthorized unofficial telephone calls may be subject to disciplinary action as well as charged for the calls.

4. Official business calls and e-mail messages are defined as those that are necessary in the interest of the government (for example, calls and e-mail messages directly related to the conduct of DOD business or having an indirect impact on DOD's ability to conduct its business).

5. Official use includes health, morale, and welfare (HMW) communications by military members and DOD employees who are deployed in remote or isolated locations for extended period of time, on official DOD business. The installation or theater commander will institute local procedures to authorize HMW communications when commercial service is unavailable, or so limited that it is considered unavailable. HMW calls may only be made during nonpeak, nonduty hours and must not exceed 5 minutes. Emergency calls may exceed this limit.

6. Authorized uses of communications systems. Authorized use includes brief communications made by DOD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DOD employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief Internet searches; e-mailing directions to visiting relatives). Such communications may be permitted provided that they:

a. Do not adversely affect the performance of official duties by the employee or the employee's organization.

b. Are of reasonable duration and frequency, and whenever possible, are made during the employee's personal time (such as during lunch, break, and other off-duty periods).

c. Are not used for activities related to the operation of a personal business enterprise.

d. In the case of long distance (toll) calls, are:

(1) Charged to the employee's home phone number or other non-Government numbers (third party call).

(2) Made to a toll-free number.

(3) Charged to the called party of a non-Government number (collect call).

(4) Charged to a personal telephone credit card.

e. Serve a legitimate public interest (such as keeping employees at their desks rather than requiring the use of commercial systems; educating DOD employees on the use of communications systems; improving the morale of employees stationed for extended periods away from home; enhancing the professional skills of DOD employees; job-searching in response to Federal Government downsizing).

7. Other prohibitions in the use of Army communications systems include the following:

a. Use of communications systems in a way that would reflect adversely on DOD or the Army (such as uses involving pornography or access to pornography web sites; chain e-mail messages; unofficial advertising, soliciting or selling via e-mail; and other uses that are incompatible with public service).

b. Use of communications systems for unlawful activities, commercial purposes or in support of "for profit" activities, personal financial gain, personal use inconsistent with DOD policy, or uses that violate other Army policies or public laws. This may include, but is not limited to, violation of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment.

c. Political transmission to include transmission which advocates the election of particular candidates for public office.

d. Misuse. Both law and Army policy prohibit, in general, the theft or other abuse of computing facilities. Such prohibitions apply to electronic mail services and include (but are not limited to): unauthorized entry, use, transfer, and tampering with the accounts and files of others and interference with the work of others and with other computing facilities.

e. Interference. Army communications systems will not be used for purposes that could reasonably be expected to cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others' use of communications. Such uses include, but are not limited to, the use of communications systems to:

(1) Create, download, store, copy, transmit, or broadcast chain letters.

(2) "Spam," that is, to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.

(3) Send a "letter-bomb," that is, to re-send the same e-mail message repeatedly to one or more recipients, to interfere with the recipient's use of e-mail.

(4) Broadcast unsubstantiated virus warnings from sources other than systems administrators.

(5) Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller populations.

(6) Guidance for telephone calls while at a temporary duty location is reflected in the Join Travel Regulations (JTR).

(7) Abuse of DOD and Army telecommunications systems, to include telephone, e-mail systems, or the Internet, may result in disciplinary action.